UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/593,561	09/20/2006	Masao Nonaka	2006_1576A	1654

52349 7590 09/29/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/593,561	NONAKA ET AL.	
	Examiner	Art Unit	
	SHIN-HON CHEN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :9/20/06, 11/30/07, 1/15/08, 2/7/08, 2/14/08, 3/27/08 and 5/1/08.

DETAILED ACTION

1. Claims 16-27 have been examined.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted to date is being considered by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 16-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marshall et al. U.S. Pat. No. 4933969 (hereinafter Marshall).

5. As per claim 16, Marshall discloses a data processing device for playing back a digital work recorded on a recording medium having also recorded (i) a plurality of record digest values generated from a plurality of data blocks constituting the digital work (Marshall: column 2 lines 27-30: plurality of MACs) and (ii) record signature data generated by applying with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values (Marshall: column 2 lines 29-30), comprising:

a verification key storing unit storing a verification key corresponding to the signature key (Marshall: column 2 lines 52-54: key);

a using unit operable to play back the digital work (Marshall: column 1 lines 66 – column 2 line 5: protect digital data);

a selecting unit operable to calculate a plurality of calculation digest values from the selected data blocks (Marshall: column 2 lines 30-45);

a calculating unit operable to calculate a plurality of calculation digest values from the selected blocks (Marshall: column 2 lines 31-35);

a reading unit operable to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values (Marshall: column 2 lines 47-55);

a generating unit operable to generate a second combination based on calculation digest values and the remaining record digest values, the second combination being the same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values (Marshall: column 2 lines 54-57: generate MACs for potentially changed or modified data for comparison);

a signature verifying unit operable to perform a signature verification by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data (Marshall: column 2 lines 47-60: generate MACs for comparison);

a use controlling unit operable to protect the digital work when the signature verification is unsuccessful (Marshall: column 1 line 68 – column 2 lines 5: protect digital data).

Marshall does not explicitly disclose a use controlling unit operable to stop the using unit from playing back the digital work when the signature verification is unsuccessful. However, it would have been obvious to one having ordinary skill in the art to apply the signature verification method disclosed by Marshall to protect and authenticate data including, but not limited to, playback of digital content.

6. As per claim 2, Marshall discloses the data processing device of claim 16. Marshall further discloses

the plurality of record digest values include a plurality of primary record digest values, each of which is generated for one of the plurality of data blocks (Marshall: column 2 lines 28-30: individual MACs for messages), and a plurality of secondary record digest values generated from two or more of the plurality of primary record digest values (Marshall: column 2 lines 30-46: MACs of blocks), and the record signature data is generated by applying, with use of the signature key, the signature generating algorithm to the first combination made of some or all of the plurality of secondary record digest values (Marshall: column 2 lines 30-46: the global MAC generated based on hierarchical structure of data),

the reading unit reads, from the recording medium, the plurality of secondary record digest values and the remaining record digest values from among the plurality of

primary record digest values (Marshall: column 2 lines 47-60: detect changes to the stored information), and

the generating unit includes:

a calculating subunit operable to calculate one or more secondary calculation digest values based on the calculation digest values and the remaining record digest values (Marshall: column 2 lines 36-45);

a combining subunit operable to generate the second combination based on the plurality of secondary record digest values and the one or more secondary calculation digest values, the second combination being the same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values (Marshall: column 2 lines 36-45: the hierarchical structure allows MACs to be generated based on different combination of data units).

7. As per claim 18, Marshall discloses the data processing device of claim 17. Marshall further discloses wherein

the digital work includes a plurality of files, each of which corresponds to one of the plurality of secondary record digest values and is constituted by two or more of the plurality of data blocks (Marshall: column 2 lines 30-45: division of data into units and subunits);

each of the plurality of secondary record digest values is generated by using primary record digest values corresponding to one-to-one with the two or more of the

plurality of data blocks constituting a file corresponding to the secondary record digest value (Marshall: column 2 lines 36-45);

the calculating subunit calculates a secondary calculation digest value, with respect to each file including at least one of the selected data blocks, by using primary record digest values corresponding to the at least one of the selected data blocks (Marshall: column 2 lines 36-45: higher level MACs are generated from lower level MACs);

the reading unit reads, with respect to each file including none of the selected data blocks, a secondary record digest value corresponding to the file, and the combining unit subunit generates the second combination by combining the calculated secondary calculation digest values and the read secondary record digest values (Marshall: column 2 lines 44-46).

8. As per claim 19, Marshall discloses the data processing device of claim 18. Marshall further discloses wherein

the plurality of record digest values are hash values each generated by a hash function (Marshall: column 2 lines 3-5: MAC),

the calculating unit applies the hash function to each of the selected data blocks in order to calculate hash values which are the calculation digest values (Marshall: column 2 lines 30-45);

the calculating subunit applies the hash function to the primary record digest values corresponding to the unselected data blocks and the calculation digest values in

order to calculate hash values which are the secondary calculation digest values (Marshall: column 2 lines 30-45: the higher level MACs).

9. As per claim 20, Marshall discloses the data processing device of claim 18. Marshall discloses method of protecting data and authenticating data based on digital signatures (Marshall: column 1 line 67 – column 2 line 5). Marshall does not explicitly disclose a warning display unit operable to display, when the digital signature work is judged as not being valid, a notice of invalidity of the digital work. However, it would have been obvious to one having ordinary skill in the art would understand data protection includes, but not limited to, controlling access based on digital signature data and display error message is access is denied because data protection using digital rights information is well known in the art and Marshall discloses using the MACs for the purpose of data protection and authentication.

10. As per claim 21, Marshall discloses the data processing device of claim 16. Marshall further discloses a second verifying unit operable to perform a signature verification by applying, with use of a verification key, a signature verification algorithm to the digital work, the area information, and the signature data (Marshall: column 2 lines 47-60). Marshall does not explicitly disclose the conventional digital rights management scheme in which access control information that includes areas permitted and the steps taken to protect playback of digital data. However, the primary access control step of this application is to rely on the signature verification method, which is disclosed by Marshall. Therefore, it would have been obvious to one having ordinary skill in the art to

incorporate the traditional digital rights management method in addition to the signature verification method because it is well known approach and it provides additional security measure to protect data.

11. As per claim 22, Marshall discloses the data processing device of claim 16. Marshall further discloses wherein

the selecting unit, the calculating unit, the reading unit and the signature verifying unit are assembled together in a single large scale integration (Marshall: column 4 lines 60-69: the security module).

12. As per claim 23, Marshall discloses the data processing device of claim 16. Marshall further discloses

wherein the reading unit reads record digest values corresponding to the selected data blocks from the recording medium (Marshall: column 22 lines 61-65: MACs are stored in directory), and

the data processing device further comprising:

a digest value verifying unit operable to make a judgment whether the plurality of record digest values recorded on the recording medium match calculation digest values (Marshall: column 2 lines 48-60); and

a third use controlling unit operable to stop the using unit from playing back the digital work when the judgment is affirmative (Marshall: column 1 line 67 – column 2 line 5: protect data and provide authentication).

13. As per claim 24, Marshall discloses a recording medium used with the data processing device of claim 16, having (i) having recorded thereon:

a digital work (Marshall: column 1 line 67 – column 2 line 1: the digital data);

a plurality of record digest values generated from a plurality of data blocks constituting the digital work (Marshall: column 2 lines 30-45); and

record signature data generated based on the plurality of record digest values (Marshall: column 2 lines 30-45); and

(ii) applying to the data processing device the digital work, the plurality of record digest values, and the record signature data (Marshall: column 2 lines 30-45: the data, the individual MACs and global MAC).

14. As per claim 25-27, claims 25-27 encompass the same scope as claims 16-24. Therefore, claims 25-27 are rejected based on the same reason set forth above in rejecting claim 25-27.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ram et al. U.S. Pub. No. 20050086241 discloses method for personal data management using MAC to detect changes to data.

Howard et al. U.S. Pat. No. 6629198 discloses generate hash value for files to determine whether file has been modified based on the hash value.

Livschitz U.S. Pat. No. 6470329 discloses one-way hash function for distributed data synchronization that determines changes made to files.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

/Shin-Hon Chen/
Examiner, Art Unit 2131